

BUNDESREPUBLIK DEUTSCHLAND



REC'D 26 NOV 2003

WIPO PCT

**Prioritätsbescheinigung über die Einreichung
einer Patentanmeldung**

Aktenzeichen: 102 50 195.5

Anmeldetag: 28. Oktober 2002

Anmelder/Inhaber: Océ Printing Systems GmbH, Poing/DE

Bezeichnung: Verfahren und Anordnung zum Authentifizieren
einer Bedieneinheit sowie Übertragen einer Au-
thentifizierungsinformation zu der Bedieneinheit

IPC: H 04 L 9/32

Die angehefteten Stücke sind eine richtige und genaue Wiedergabe der ursprüng-
lichen Unterlagen dieser Patentanmeldung.

München, den 5. November 2003
Deutsches Patent- und Markenamt
Der Präsident
Im Auftrag

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH
RULE 17.1(a) OR (b)

**Verfahren und Anordnung zum Authentifizieren einer
Bedieneinheit sowie Übertragen einer
Authentifizierungsinformation zu der Bedieneinheit**

- 5 Die Erfindung betrifft ein Verfahren und eine Anordnung zum Erzeugen von Authentifizierungsinformationen durch die eine Datenverarbeitungsanlage eine Authentifizierung einer Bedieneinheit durchführt. Ferner betrifft die Erfindung ein Verfahren und eine Anordnung zur Authentifizierung einer Bedieneinheit eines elektrofotografischen Drucker- oder Kopiersystems.
- 10 Bekannte elektrofotografische Drucker und Kopierer haben Kommunikationsschnittstellen, über die Bedieneinheiten und Wartungscomputer mit dem Drucker oder Kopierer zum Bedienen, zur Diagnose und zur Wartung verbunden werden können. Insbesondere mit Hilfe der Wartungscomputer können sicherheitsrelevante Einstellwerte des Druckers oder Kopierers geändert werden. Werden solche Änderungen von nicht ausreichend qualifizierten Bedienpersonen oder z.B. über eine Netzwerkverbindung, durch Unberechtigte durchgeführt, kann eine erhebliche Qualitätsverschlechterung und eine Schädigung bzw. Zerstörung von Baugruppen des Druckers oder Kopierers erfolgen.
- 15 Bei bekannten Druckern und Kopierern sind mehrere sogenannte Benutzerstufen vorgesehen, wobei eine Bedienperson eine Benutzerstufe auswählen kann und seine Berechtigung zur Auswahl dieser Benutzerstufe durch eine Passworteingabe bestätigt. Ferner besteht bei bekannten Druckern und Kopierern durch ungesicherte Zugriffe die Möglichkeit, dass unberechtigte Personen Informationen über den Aufbau und die Steuerungsstruktur des Druckers oder Kopierers mit Hilfe der Kommunikationsschnittstelle des Druckers oder Kopierers erhalten. Auch Systemparameter, wie Zählerstände des Druckers oder Kopierers, die gegebenenfalls auch für Abrechnungszwecke genutzt werden, können über die Kommunikationsschnittstelle bekannter Drucker oder Kopierer manipuliert werden.
- 20
- 30
- 35

Aus dem Europäischen Patent EP 0 513 549 A2 ist eine Anordnung zum Steuern und zum Übertragen von Daten zwischen einem Host-Computer und einer Kopierersteuerung bekannt, wobei die Kommunikation erst bei erfolgter Identifizierung des Host-Computers mit Hilfe eines Passwortes erfolgt ist. Ferner ist eine Steuereinheit zur Kommunikationssteuerung vorgesehen.

Aus dem Patent US 5,077,795 ist ein elektronisches Drucksystem bekannt, bei dem mit Hilfe eines Benutzerprofils für jeden Benutzer die Sicherheit von Nutzerdaten und Nutzerprogrammen sichergestellt ist. Die Benutzerprofile werden von einem Sicherheits-Administrator vor Ort oder von einem entfernten Ort aus verwaltet.

Jedoch bieten die bekannten Zugriffsverfahren nur einen unzureichenden Schutz von druckerinternen Daten und Einstellwerten. Insbesondere besteht bei Passwörtern ein erhebliches Sicherheitsrisiko darin, dass Passwörter mit Hilfe von Programmmodulen ausgespäht werden können, die Tastatureingaben mitschneiden. Ferner besteht ein Sicherheitsrisiko bei Passwörtern darin, dass die Passwörter dem jeweiligen Benutzer zugestellt werden müssen, wobei oft nicht sichergestellt werden kann, dass Unberechtigte Kenntnis der Passwörter bei der Übertragung und/oder Zustellung der Passwörter erhalten. Auch ist bei Passwörtern nicht sichergestellt, dass berechtigte Personen die Passwörter nicht an unberechtigte Personen weitergeben. Ein wirksamer lokaler Schutz bekannter Drucker oder Kopierer konnte nur durch das Verhindern eines physikalischen Zugriffs von unberechtigten Personen auf die Kommunikationsschnittstelle des Druckers oder Kopierers erfolgen. Jedoch ist dann auch erforderlich, dass die Druckdaten nicht über ein Netzwerk zum Drucker übertragen werden, das auch mit globalen Netzwerken, wie dem Internet, verbunden ist, über das auch unbefugte Personen Zugriff auf den Drucker erhalten. Diese Maßnahmen verhindern jedoch auch, dass eine Fernwartung, Ferndiagnose oder Fernbedienung des Druckers

durch Servicespezialisten durchgeführt werden kann, die nicht vor Ort am Drucker sind.

5 Aufgabe der Erfindung ist es, ein Verfahren und eine Anordnung anzugeben, durch die eine einfache Authentifizierung einer Datenverarbeitungsanlage möglich ist.

10 Die Aufgabe wird für ein Verfahren zur Authentifizierung einer Datenverarbeitungsanlage mit den Merkmalen des Patentanspruchs 1 gelöst. Vorteilhafte Weiterbildungen der Erfindung sind in den abhängigen Patentansprüchen angegeben.

15 Durch ein Verfahren zur Authentifizierung einer Datenverarbeitungsanlage mit den Merkmalen des Patentanspruchs 1 wird erreicht, dass der zweiten Datenverarbeitungsanlage auf sehr sichere Art und Weise die zweiten Daten zugeführt werden, wobei die zweite Datenverarbeitungsanlage mit Hilfe der zweiten Daten Authentifizierungsinformationen erzeugt, mit denen vorzugsweise automatisch ohne Eingriff einer Bedienerperson
20 eine Authentifizierungsprozedur durchführbar ist.

Ein zweiter Aspekt der Erfindung betrifft eine Anordnung zur Authentifizierung einer Datenverarbeitungsanlage. Eine erste Datenverarbeitungsanlage erzeugt erste Informationen. Die ersten Informationen werden einer zweiten Datenverarbeitungsanlage einer Bedieneinheit zugeführt. Die zweite Datenverarbeitungsanlage erzeugt mit Hilfe der ersten Informationen und einer in der zweiten Datenverarbeitungsanlage enthaltenen weiteren Information erste Daten. Die Anordnung enthält eine
30 Datenleitung, über die erste Daten von der ersten Datenverarbeitungsanlage zur zweiten Datenverarbeitungsanlage übertragbar sind. Die erste Datenverarbeitungsanlage erzeugt abhängig von den ersten Daten zweite Daten. Die zweiten Daten sind über die Datenleitung von der ersten Datenverarbeitungsanlage
35 zur zweiten Datenverarbeitungsanlage übertragbar. Die zweite Datenverarbeitungsanlage erzeugt mit Hilfe der zweiten Daten

Authentifizierungsinformationen zur Authentifizierung der zweiten Datenverarbeitungsanlage.

- 5 Durch diese erfindungsgemäße Anordnung wird erreicht, dass das Erzeugen und Übertragen der zweiten Daten zum Erzeugen der Authentifizierungsinformationen durch die zweite Datenverarbeitungsanlage einfach und ohne aufwendige Benutzereingriffe durchführbar ist. Ferner ist, insbesondere dadurch, dass die zweite Datenverarbeitungsanlage mit Hilfe der zweiten Daten die Authentifizierungsinformationen erzeugt, eine Authentifizierung der zweiten Datenverarbeitungsanlage durch eine weitere Datenverarbeitungsanlage und/oder die erste Datenverarbeitungsanlage einfach möglich.
- 10
- 15 Ein dritter Aspekt der Erfindung betrifft ein Verfahren zur Authentifizierung einer Bedieneinheit eines elektrofotografischen Druck- oder Kopiersystems. In einer ersten Datenverarbeitungsanlage der Bedieneinheit werden erste Daten gespeichert. Die erste Datenverarbeitungsanlage erzeugt mit Hilfe
- 20 der ersten Daten eine Authentifizierungsinformation. Mit Hilfe von Authentifizierungsdaten wird die Authentifizierungsinformation zu einer zweiten Datenverarbeitungsanlage des Druck- oder Kopiersystems übertragen. Die Authentizität der ersten Datenverarbeitungsanlage wird durch die zweite Datenverarbeitungsanlage überprüft. Mit Hilfe der Authentifizierungsdaten werden durch die zweite Datenverarbeitungsanlage Zugriffsrechte der ersten Datenverarbeitungsanlage festgelegt.
- 30 Durch dieses erfindungsgemäße Verfahren wird erreicht, dass eine Authentifizierung der Bedieneinheit und das Festlegen der Zugriffsrechte der Bedieneinheit sehr einfach möglich ist. Aufwendige Bedieneingriffe einer Bedienperson sind zur Authentifizierung der Bedieneinheit nicht erforderlich.
- 35 Ein vierter Aspekt der Erfindung betrifft eine Anordnung zum Authentifizieren einer Bedieneinheit eines elektrofotografi-

schen Druck- oder Kopiersystems. Erste Daten sind in einer ersten Datenverarbeitungsanlage der Bedieneinheit gespeichert. Die erste Datenverarbeitungsanlage erzeugt mit Hilfe der ersten Daten eine Authentifizierungsinformation. Die
5 erste Datenverarbeitungsanlage überträgt Authentifizierungsdaten zu einer zweiten Datenverarbeitungsanlage des Druck- oder Kopiersystems, wobei die Authentifizierungsdaten die Authentifizierungsinformation enthalten. Die zweite Datenverarbeitungsanlage überprüft die Authentizität der ersten Da-
10 tenverarbeitungsanlage, wobei die zweite Datenverarbeitungsanlage mit Hilfe der Authentifizierungsdaten Zugriffsrechte der ersten Datenverarbeitungsanlage festlegt. Durch diese erfindungsgemäße Anordnung wird erreicht, dass eine Authentifizierung der Bedieneinheit sehr einfach durch die Bedienein-
15 heit des Druck- oder Kopiersystems durchgeführt wird. Eingriffe von einer Bedienperson sind für eine solche Authentifizierung nicht zwingend erforderlich. Ferner wird durch diese Anordnung erreicht, dass eine sehr sichere Authentifizierung der Bedieneinheit durchgeführt wird und Fremdzugriffe
20 auf die Datenverarbeitungsanlage des Druck- oder Kopiersystems verhindert werden.

Zum besseren Verständnis der vorliegenden Erfindung wird im Folgenden auf die in den Zeichnungen dargestellten bevorzugten Ausführungsbeispiele Bezug genommen, die an Hand spezifischer Terminologie beschrieben sind. Es sei jedoch darauf hingewiesen, dass der Schutzzumfang der Erfindung dadurch nicht eingeschränkt werden soll, da derartige Veränderungen und weitere Modifizierungen an den gezeigten Vorrichtungen
30 und/oder dem Verfahren sowie derartige weitere Anwendungen der Erfindung, wie sie darin aufgezeigt sind, als übliches derzeitiges oder künftiges Fachwissen eines zuständigen Fachmannes angesehen werden. Die Figuren zeigen Ausführungsbeispiele der Erfindung, nämlich:

Figur 1 ein Blockschaltbild eines Systems zum Erzeugen und Übertragen eines Schlüssels zur Authentifizierung eines Service- und Wartungscomputers;

5 Figur 2 eine Bedienoberfläche zum Anfordern des Schlüssels bei einem Autorisierungs-Server;

Figur 3 ein Blockschaltbild zur Authentifizierung des Service- und Wartungscomputers durch einen Drucker;
10 und

Figur 4 ein Ausgabefenster mit einer Testmeldung, die bei einer fehlerhaften Autorisierung ausgegeben wird.

15 In Figur 1 ist ein System 10 zum Erzeugen und Übertragen eines Schlüssels 12 dargestellt, der zur Authentifizierung eines Service- und Wartungscomputers 14 durch eine weitere nicht dargestellte Datenverarbeitungseinheit eines Druckers dient. Das System 10 enthält einen Autorisierungs-Server 16,
20 der über eine Netzwerkverbindung 18 mit dem Service- und Wartungscomputer verbindbar ist. Das Erzeugen und Übertragen des Schlüssels 12 wird auch als Freischaltungsverfahren des Service- und Wartungscomputers 14 bezeichnet. Für diese Freischaltungsverfahren ist eine Datenverbindung, z.B. über Netzwerk 18, zwischen dem Service- und Wartungscomputer 14 und dem Autorisierungs-Server 16 erforderlich.

Der Autorisierungs-Server 16 erzeugt eine sogenannte Transaktionsnummer (TAN). Die Transaktionsnummer ist eine
30 Ziffern- und/oder Buchstabenfolge, die eine Bedienperson am Service- und Wartungscomputer zum Durchführen der Freischaltungsverfahren eingeben muss. Die vom Autorisierungs-Server 16 erzeugte Transaktionsnummer wird der Bedienperson per Post oder per E-Mail zugesendet. Die Bedienperson ist
35 vorzugsweise ein Servicetechniker des Druckerherstellers, der einen portablen Computer, ein sogenanntes Notebook, als Service- und Wartungscomputer 14 besitzt. Im Folgenden wird der Service- und Wartungscomputer 14 des Servicetechnikers

tungscomputer 14 des Servicetechnikers als Service-Notebook bezeichnet.

Der Servicetechniker startet auf dem Service-Notebook 14 ein
5 Programmmodul zum Durchführen der Freischaltungsverfahren,
nachdem er per Post oder E-Mail die Transaktionsnummer erhalten
hat. Der Servicetechniker gibt mit Hilfe einer Bedien-
oberfläche die Transaktionsnummer ein und startet anschlie-
ßend den Freischaltungsverfahren. Das Programmmodul ermittelt
10 ein vorbestimmtes Hardwaremerkmal, z.B. die Seriennummer des
Prozessors oder eines Netzwerkadapters. Ein solches Hardware-
merkmal wird auch als "Fingerprint" des Service-Notebooks 14
bezeichnet. Über die Netzwerkverbindung 18 wird die Serien-
nummer und die Transaktionsnummer zum Autorisierungs-Server
15 16 übertragen. Der Autorisierungs-Server 16 überprüft die
Gültigkeit der Transaktionsnummer und legt aufgrund der
Transaktionsnummer eine Berechtigungsstufe des Service-
Notebooks 14 fest, die dann bei einer späteren Verbindung des
Service-Notebooks 14 mit einem Drucker die Zugriffsrechte des
20 Service-Notebooks 14 auf die Steuereinheiten und Datenbasen
des Druckers festlegt.

Der Autorisierungs-Server 16 legt weiterhin ein Gültigkeits-
datum fest, bis zu dem eine Autorisierung mit Hilfe des zu
erzeugenden Schlüssels 12 durch einen Drucker möglich ist.
Vorzugsweise ist auch ein Zeitraum festgelegt, in dem mit
Hilfe der gesendeten Transaktionsnummer ein Service-Notebook
14 freigeschaltet werden kann. Mit Hilfe des übertragenen
Hardwaremerkmals, dem Gültigkeitsdatum und der Berechtigungs-
30 stufe erzeugt der Autorisierungs-Server 16 einen sogenannten
Schlüssel 12, der diese Angaben vorzugsweise in codierter
Form enthält und/oder durch den zumindest eine Überprüfung
dieser Angaben möglich ist. Der erzeugte Schlüssel 12 wird
über das Netzwerk 18 zum Service-Notebook 14 übertragen,
35 wobei der Schlüssel 12 in einem Speicherbereich des Service-
Notebooks 14 gespeichert wird.

Mit Hilfe des Systems 10 ist somit eine Freischaltungsverfahren zum Freischalten des Service-Notebooks 14 erfolgt. Der durch diese Freischaltungsverfahren im Service-Notebook 14 gespeicherte Schlüssel 12 enthält das Hardwaremerkmal, das
5 Verfallsdatum und die Zugriffsrechte des Service-Notebooks 14 in verschlüsselter Form.

Bei anderen Ausführungsbeispielen sind zumindest das Hardwaremerkmal, das Verfallsdatum und die Zugriffsrechte mit
10 Hilfe des Schlüssels 12 überprüfbar. Die Transaktionsnummer kann bei weiteren Ausführungsbeispielen auch von einer separaten Institution erzeugt werden. Die Transaktionsnummer muss dann dem Servicetechniker zur Eingabe in das Service-Notebook 14 übersandt und dem Autorisierungs-Server 16 eingegeben
15 werden. Die Netzwerkverbindung 18 ist nach Figur 1 eine Verbindung über ein Wide Area Network, wie z.B. dem Internet. Wird eine solche Verbindung über das Internet gewählt, so erfolgt die Datenübertragung vorzugsweise mit Hilfe eines gesicherten Übertragungskanal.

20 Alternativ kann bei anderen Ausführungsbeispielen eine Punkt-zu-Punkt-Verbindung, z.B. mit Hilfe von Modems, über ein öffentliches Telefonnetz übertragen werden. Um die Übertragungssicherheit zu erhöhen, können zur Datenübertragung weiterhin bekannte Verschlüsselungsverfahren zur Datenübertragung genutzt werden. Mit Hilfe des Systems 10 ist es weiterhin möglich, dass ein Servicetechniker das Service-Notebook 14 von einem beliebigen, mit dem Netzwerk 18 verbindbaren Ort aus freischalten kann. So ist es z.B. auch möglich, das Service-Notebook 14 von einem Telefonanschluss eines Kunden aus
30 oder von einem beliebigen anderen Telefonanschluss aus freizuschalten.

Ist die Gültigkeitsdauer des Schlüssels 12 abgelaufen, so ist
35 eine wiederholte Freischaltung des Service-Notebooks 14 erforderlich. Zum wiederholten Freischalten wird dieselbe Freischaltungsverfahren nochmals durchgeführt, wie bereits zuvor

für die erste Freischaltung des Service-Notebooks 14 beschrieben.

5 Für unterschiedliche Service-Notebooks mit gleicher Berechtigungsstufe werden durch den Autorisierungs-Server 16 unterschiedliche Schlüssel 12 erzeugt und zugewiesen. Aus diesen unterschiedlichen Schlüsseln 12 ist jedoch jeweils eindeutig die Berechtigungsstufe und der Gültigkeitszeitraum ermittelbar, ohne dass der Schlüssel 12 selbst einer Datenverarbeitungsanlage des Druckers bekannt sein muss, die die Authentizität des Service-Notebooks 14 überprüft. Dadurch wird erreicht, dass es nicht erforderlich ist, allen Druckern mitzuteilen, welche Service-Notebooks 14 der Servicetechniker und welche weiteren Bedieneinheiten eine Berechtigung zum Zugriff auf die Datenbasis und/oder die Steuereinheiten des jeweiligen Druckers haben. Ein solches Service-Notebook 14 wird als Bedieneinheit mit einem Drucker lokal oder über eine Netzwerkverbindung 18 verbunden, wobei mit Hilfe des Service-Notebooks 14 sowohl Einstellwerte des Druckers ausgelesen als auch geänderte Einstellwerte zum Drucker übertragen werden können, der Drucker mit Hilfe des Service-Notebooks 14 bedient werden kann und eine Diagnose des Druckers oder von Baugruppen des Druckers mit Hilfe des Service-Notebooks 14 durchgeführt wird.

Durch die Druckersoftware bzw. durch die Firmware des Druckers ist für jeden einzelnen Parameter festgelegt, bis zu welcher Berechtigungsstufe ein Lese- und/oder Schreibzugriff auf diesen Einstellparameter gestattet ist. Vorzugsweise werden die Schreibzugriffe auf Einstellparameter nur Benutzern mit einer hohen Berechtigungsstufe gestattet.

35 In Figur 2 ist eine Bedienoberfläche 20 zum Freischalten des Service-Notebooks 14 dargestellt. Die Bedienoberfläche 20 wird mit dem von dem Servicetechniker auf dem Service-Notebook 14 gestarteten Programmmodul zum Freischalten des Service-Notebooks 14 erzeugt und auf einer Anzeigeeinheit des

Service-Notebooks 14 ausgegeben. Mit Hilfe dieser Bedienoberfläche 20 kann die Bedienperson die Art der Verbindung zum Autorisierungs-Server 16 auswählen. In einem Ein- und Ausgabefeld 22 kann die Bedienperson die Netzwerkadresse oder die Internetadresse des Autorisierungs-Servers 16 auswählen oder eintragen, wenn das Service-Notebook 14 über eine Netzwerkverbindung des World Wide Web des Internets mit dem Autorisierungs-Server 16 verbunden ist. Mit Hilfe eines Auswahlfeldes 24 kann die Bedienperson alternativ eine Punkt-zu-Punkt-Verbindung des Service-Notebooks 14 mit dem Autorisierungs-Server 16 einstellen, wenn das Service-Notebook 14 und der Autorisierungs-Server 16 z.B. über Modems mit Hilfe eines Telefonnetzes verbindbar sind. Für eine solche Punkt-zu-Punkt-Verbindung kann die Bedienperson im Eingabeabschnitt 26 die erforderlichen Daten zum Verbindungsaufbau der Punkt-zu-Punkt-Verbindung eingeben. Diese Daten betreffen insbesondere einen Loginnamen und ein Passwort zum Aufbau der Verbindung und eine Telefonnummer, über die der Autorisierungs-Server über das Telefonnetz erreichbar ist. Ferner ist ein zu nutzendes Protokoll auswählbar.

Der Abschnitt 26 enthält weiterhin ein Ausgabefeld, in dem der Verbindungsstatus angezeigt wird. Mit Hilfe einer grafischen Funktionstaste 28 kann eine Verbindung über das Telefonnetz hergestellt werden. Mit Hilfe der grafischen Funktionstaste 30 kann eine bestehende Verbindung unterbrochen werden, wobei mit Hilfe der grafischen Funktionstaste 32 sowohl der Verbindungsaufbau als auch der Verbindungsabbau unterbrochen werden kann. In einem Eingabefeld 34 ist die übermittelte Transaktionsnummer (TAN) einzugeben. Nach der Eingabe der Transaktionsnummer kann die Bedienperson mit Hilfe der grafischen Funktionstaste 36 den Registrierungsvorgang beim Autorisierungs-Server 16 starten, wobei das Programmmodul sowohl die Transaktionsnummer als auch die Nummer des Prozessors des Service-Notebooks 14 zum Autorisierungs-Server 16 überträgt. Das Programmmodul enthält spezielle Programmelemente zum Ermitteln der Seriennummern

des Prozessors.

Wie bereits in Zusammenhang mit Figur 1 beschrieben, ermittelt der Autorisierungs-Server 16 mit Hilfe der Seriennummer
5 des Prozessors und weiteren Informationen einen Schlüssel 12, nachdem er die Gültigkeit der Transaktionsnummer überprüft hat. Nach dem Erzeugen des Schlüssels 12 wird dieser zum Service-Notebook 14 übertragen. Der Schlüssel 12 wird in einem dafür vorgesehenen Speicherbereich des Service-Note-
10 books 14 gespeichert. Nachdem der Schlüssel 12 erfolgreich zum Service-Notebook 14 übertragen worden ist, wird die grafische Funktionstaste 38 aktiviert dargestellt, dass das Service-Notebook 14 erfolgreich freigeschaltet worden ist. Durch Aktivieren der grafischen Funktionstaste 38 wird der
15 Freischaltungsverfahren abgeschlossen und die Abarbeitung des Programmmoduls zur Freischaltung beendet.

In Figur 3 ist ein Blockschaltbild zur Authentifizierung des Service-Notebooks 14 durch einen Drucker 40 dargestellt. Das
20 Service-Notebook 14 ist über eine Netzwerkverbindung 42 mit dem Drucker 40 verbunden. Wie bereits in Zusammenhang mit den Figuren 1 und 2 erläutert, ist ein Schlüssel 12 im Service-Notebook 14 gespeichert, wobei der Schlüssel 12 Informationen über die Seriennummer des Prozessors, die Gültigkeitsdauer des Schlüssels 12 und die Zugriffsrechte des Service-Notebooks 14 enthält. Vorzugsweise sind diese Informationen codiert im Schlüssel 12 enthalten. Alternativ sind mit Hilfe des Schlüssels 12 diese Informationen zumindest überprüfbar.

30 Bevor das Service-Notebook 14 Zugriff auf Einstellparameter und Diagnosefunktionen des Druckers 40 erhält, führt der Drucker 40 eine Autorisierung des Service-Notebooks 14 durch. Dazu wird durch ein Programmmodul des Druckers über das Netzwerk 42 das Vorhandensein des Schlüssels 12 auf dem Service-
35 Notebook 14 und die Berechtigungsstufe des Service-Notebooks 14 ermittelt. Vorzugsweise erfolgt die Autorisierung durch den Drucker 40 mit Hilfe eines Challenge- und Response-

Verfahrens. Dabei überträgt der Drucker 40 eine Zufallszahl zum Service-Notebook 14. Das Service-Notebook 14 führt mit der Zufallszahl abhängig vom Schlüssel 12 eine nicht umkehrbare mathematische Rechenoperation aus. Das Ergebnis dieser

5 Rechenoperation wird über die Netzwerkverbindung 42 zum Drucker 40 übertragen. Der Drucker 40 überprüft das Rechenergebnis, indem er eine mathematischen Rechenoperation ausführt, die ebenfalls zu demselben Ergebnis führt. Stimmen die beiden Rechenergebnisse überein, so ist die Authentifizierung des

10 Service-Notebooks 14 durch den Drucker 40 erfolgt.

Wie bereits erwähnt, ist für jeden Einstellparameter des Druckers 40 im Drucker 40 festgelegt, ob Nutzer mit einer vorbestimmten Berechtigungsstufe Lese- und/oder Schreibzugriffe auf den Wert des Einstellparameters haben. Ein solcher Nutzer ist z.B. das Service-Notebook 14. Nach erfolgter Authentifizierung des Service-Notebooks 14 überträgt der Drucker 40 Daten zum Erzeugen einer grafischen Benutzeroberfläche zum Bedienen, zur Konfiguration und zur Wartung des

15 Druckers 40 zum Service-Notbook 14. Die übertragenen Daten werden mit Hilfe eines Browser-Programmoduls durch das Service-Notebook verarbeitet. Die grafische Benutzeroberfläche enthält vorzugsweise Bedienoberflächen, wobei anzuzeigende Bedienoberflächen insbesondere mit Hilfe von Menüeinträgen

20 auswählbar sind.

Die grafische Benutzeroberfläche und die Bedienoberflächen sind vorzugsweise so ausgeführt, dass sie durch den Drucker 40 automatisch an die Berechtigungsstufe des Service-

30 Notebooks 14 angepasst wird. Ist das Service-Notebook 14 aufgrund der zugewiesenen Berechtigungsstufe nicht befugt, Lese- und/oder Schreibzugriffe auf den Einstellwert eines Einstellparameters durchzuführen, so wird dieser Einstellwert nicht bzw. nur deaktiviert dargestellt. Hat das Service-

35 Notebook 14 nicht die Berechtigung, eine bestimmte Diagnosefunktion auszuführen, so wird diese Diagnosefunktion nicht mit über die Bedienoberfläche und/oder über Menüeinträge der

Bedienoberfläche angeboten, d.h. nicht angezeigt. Somit ist das Bedienen der Bedienoberfläche bei niedrigen Berechtigungsstufen einfacher und übersichtlicher.

5 Mit Hilfe einer solchen Autorisierungsprozedur, wie sie in Zusammenhang mit den Figuren 1 bis 3 beschrieben worden ist, ist es einfach möglich, versehentliche oder vorsätzliche Manipulationen und Falscheinstellungen von Einstellparametern des Drucksystems zu verhindern. Der Zugriff des Service-
10 Notebooks 14 auf den Drucker ist dabei sowohl über eine direkte Datenleitung vor Ort als auch über eine Netzwerkverbindung, z.B. über das Internet oder ein Telefonnetz, von einem entfernten Ort aus möglich. Somit ist eine Fernwartung, Bedienung und Ferndiagnose sehr einfach möglich.

15 Wird die Benutzeroberfläche zum Bedienen, zur Konfiguration und zur Diagnose des Druckers 40 vom Drucker 40 über das Netzwerk 42 zum Service-Notebook 14 übertragen und auf diesem mit Hilfe eines Anzeigeprogrammmoduls, z.B. mit Hilfe eines
20 Browsers angezeigt, so benötigt das Service-Notebook 14 lediglich Software zum Anfordern und Verwalten des Schlüssels 12, die zusätzlich zu der Standardsoftware des Service-Notebooks 14 in einem Speicherbereich des Service-Notebooks 14 gespeichert und von diesem abgearbeitet werden muss. Die Standardsoftware des Service-Notebooks 14 umfasst zumindest ein Betriebssystem und ein Browserprogrammmodul.

Vorzugsweise enthält das Browserprogrammmodul eine Java-
Runtime-Programmumgebung, eine sogenannte Java-Runtime-
30 Environment. Mit Hilfe dieser Java-Runtime-Environment ist das Abarbeiten von Java-Programmelementen, sogenannten Java-Applets sehr einfach möglich. Mit Hilfe der Java-Applets können umfangreiche Bedien-, Diagnose- und Konfigurationsfunktionen sowie eine grafische Benutzeroberfläche erzeugt
35 werden, die über das Browserprogrammmodul ausgegeben werden. Ein Übertragen und Überprüfen von Passwörtern ist nicht erforderlich. Insbesondere beinhaltet ein solches Passwort die

Gefahr, dass z.B. bei einer Wochenend- oder Urlaubsvertretung des Servicetechnikers oder einer Bedienperson das Passwort an einen anderen Servicetechniker oder an eine andere Bedienperson weitergegeben wird. Oft werden diese Passwörter auch
5 notiert und können so zu nicht berechtigten Personen gelangen.

Mit Hilfe der erfindungsgemäßen Authentifizierung des Service-Notebooks 14 enthält das Service-Notebook 14 alle zur
10 Authentifizierung des Service-Notebooks 14 erforderlichen Daten. Bei einer Urlaubs- oder Wochenendvertretung wird einfach einem anderen Servicetechniker oder einer anderen Bedienperson das Service-Notebook 14 übergeben. Der vertretende Servicetechniker oder die vertretende Bedienperson erhält
15 keinerlei Informationen, mit denen es möglich ist, nach Rückgabe des Service-Notebooks 14 mit einem anderen Service-Notebook oder einer anderen Datenverarbeitungsanlage Zugriff auf den Drucker 40 zu erhalten.

20 In Figur 4 ist ein Ausgabefenster mit einer Textmeldung dargestellt, das auf dem Service-Notebook 14 bei nicht erfolgter Freischaltung und bei abgelaufener Freischaltung ausgegeben wird. Mit Hilfe dieser Textmeldung wird der Servicetechniker darüber informiert, dass das Service-Notebook 14 nicht freigeschaltet ist und er keinen Zugriff auf Servicewerkzeuge, Diagnosewerkzeuge und Dokumentationen hat. Mit Hilfe der grafischen Funktionstaste 44 kann die Bedienperson das Programmmodul zur Freischaltung des Service-Notebooks 14 starten, wodurch die in Figur 2 dargestellte Bedienoberfläche
30 ausgegeben wird. Jedoch ist eine solche Freischaltung, wie in Zusammenhang mit Figur 2 bereits erläutert, nur möglich, wenn die Bedienperson eine gültige Transaktionsnummer hat. Durch Aktivieren der grafischen Funktionstaste 46 wird das Programmmodul zum Freischalten nicht gestartet und dem Servicetechniker stehen beim Service-Notebook 14 die eine Berechtigungsstufe erfordernden Service- und Diagnosewerkzeuge sowie
35 eine Servicedokumentation nicht zur Verfügung.

Alternativ zur Seriennummer des Prozessors kann auch eine sogenannte MAC-Adresse der im Service-Notebook 14 enthaltenen Netzwerkkarte als Hardwaremerkmal genutzt werden. Die MAC-Adresse wird auch als Ethernet-Adresse bezeichnet. Die MAC-Adresse ist eine weltweit eindeutige Kennung eines Netzwerkadapters. Sie wird in Schicht 2 des OSI-Modells zur Adressierung genutzt. Die MAC-Adresse ist in einem ROM-Speicher des Netzwerkadapters gespeichert und nicht mit Hilfe von Programmmodulen des Service-Notebooks 14 änderbar. Die MAC-Adresse ist sechs Byte lang, in denen verschlüsselt der Hersteller und die Seriennummer des jeweiligen Netzwerkadapters enthalten ist. Die MAC-Adresse ist mit bekannten Programmmodulen auslesbar. Die MAC-Adresse dient somit zur eindeutigen Identifizierung des Service-Notebooks 14.

Weiterhin ist es vorteilhaft, mehrere Benutzergruppen vorzusehen, denen jeweils eine Berechtigungsstufe zugeordnet ist. Mit einer solchen Authentifizierung können auch Kundendaten, wie z.B. Overlays, Zeichensätze und andere Ressourcen, gegen unberechtigtes Auslesen oder Ändern geschützt werden. Dabei kann auch eine Autorisierung von anderen internen und externen Bedieneinheiten des Druckers durchgeführt werden, bevor diese Bedieneinheiten Zugriff auf die Einstellparameter und Bedienfunktionen des Druckers erhalten. Dadurch wird auch eine unberechtigte Bedienung des Druckers 40, die z.B. über ein Netzwerk erfolgen kann, an dem der Drucker 40 angeschlossen ist, verhindert werden. Vorzugsweise wird dabei auch ein Verfahren zur Kryptografie genutzt, mit dem Informationen verschlüsselt und anschließend entschlüsselt werden, insbesondere ein asymmetrisches oder ein symmetrisches Verschlüsselungsverfahren. Weiterhin kann der Schlüssel 12 einen Legitimationscode enthalten. Der Schlüssel 12 ist vorzugsweise ein Public-Key oder ein Private-Key. Alternativ kann anstatt des Schlüssels 12 auch eine Signatur genutzt werden.

- Obgleich in den Zeichnungen und der vorhergehenden Beschreibung bevorzugte Ausführungsbeispiele aufgezeigt und detailliert beschrieben sind, sollte dies als rein beispielhaft und die Erfindung nicht einschränkend angesehen werden. Es wird
- 5 darauf hingewiesen, dass nur die bevorzugten Ausführungsbeispiele dargestellt und beschrieben sind und sämtliche Veränderungen und Modifizierungen, die derzeit und künftig im Schutzzumfang der Erfindung liegen, geschützt werden sollen.

Bezugszeichenliste

	10	System
	12	Schlüssel
5	14	Service-Notebook
	16	Autorisierungs-Server
	18, 42	Netzwerk/Netzwerkverbindung
	20	Bedienoberfläche
	22	Ein- und Ausgabefeld
10	24	Auswahlfeld
	26	Abschnitt zur Ein- und Ausgabe
	28, 30, 32, 36, 38	grafische Funktionstasten
	34	Eingabefeld
	40	Drucker
15	44, 46	grafische Funktionstasten

Patentansprüche

- 5 1. Verfahren zur Authentifizierung einer Datenverarbeitungs-
anlage,

bei dem mit Hilfe einer ersten Datenverarbeitungsanlage
(16) eine erste Information erzeugt wird, die einer zweiten
Datenverarbeitungsanlage (14) einer Bedieneinheit
10 zugeführt wird,

erste Daten von der zweiten Datenverarbeitungsanlage (14)
zur ersten Datenverarbeitungsanlage (16) über eine Daten-
leitung übertragen werden, wobei die ersten Daten von der
15 zweiten Datenverarbeitungsanlage (14) mit Hilfe der ers-
ten Information und einer in der zweiten Datenverarbei-
tungsanlage (14) enthaltenen weiteren Information erzeugt
werden,

20 mit Hilfe der ersten Datenverarbeitungsanlage (16) abhän-
gig von den ersten Daten zweite Daten erzeugt werden, die
von der ersten Datenverarbeitungsanlage (16) zur zweiten
Datenverarbeitungsanlage (14) über die Datenleitung über-
tragen werden,

und bei dem durch die zweite Datenverarbeitungsanlage
(14) mit Hilfe der zweiten Daten Authentifizierungsinfor-
mationen zur Authentifizierung der zweiten Datenverarbei-
tungsanlage (14) erzeugt werden.

30

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass
die weiteren Informationen ein Hardwaremerkmal der zwei-
ten Datenverarbeitungsanlage (14) enthalten.
- 35 3. Verfahren nach Anspruch 2, dadurch gekennzeichnet, dass
mit Hilfe der zweiten Daten überprüft wird, ob die zweite

Datenverarbeitungsanlage (14) das Hardwaremerkmal enthält.

- 5 4. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass die zweiten Daten ein Verfallsdatum und Informationen enthalten, durch die Zugriffsrechte der zweiten Datenverarbeitungsanlage (14) festgelegt werden.
- 10 5. Verfahren nach Anspruch 4, dadurch gekennzeichnet, dass die Zugriffsrechte mit Hilfe einer Berechtigungsstufe zugewiesen werden.
- 15 6. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass die zweiten Daten verschlüsselt übertragen werden.
- 20 7. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass die Datenleitung eine Netzwerkverbindung, insbesondere eine gesicherte Internetverbindung ist.
8. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass die Datenverbindung eine Punkt-zu-Punkt-Verbindung ist.
9. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass die zweiten Daten einen Schlüssel (12) enthalten.
- 30 10. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass die Authentizität der zweiten Datenverarbeitungsanlage (14) von einer dritten Datenverarbeitungsanlage (40) überprüft wird, die in einem elektrofotografischen Druck- oder Kopiersystem enthalten ist.
- 35

11. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass die ersten Informationen eine Transaktionsnummer enthalten.
- 5 12. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass die ersten Informationen per E-Mail oder per Post versendet werden.
- 10 13. Verfahren nach Anspruch 12, dadurch gekennzeichnet, dass die der ersten Datenverarbeitungsanlage (16) zugeführten ersten Informationen über eine Eingabeeinheit der ersten Datenverarbeitungsanlage (16) eingegeben werden.
- 15 14. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass die zweite Datenverarbeitungsanlage (14) eine Bedieneinheit, insbesondere zur Konfiguration, Wartung und Bedienung, eines elektrofotografischen Druck- oder Kopiersystems ist, wobei eine dritte Datenverarbeitungsanlage (40) des Druck- oder Kopiersystems die Authentizität der zweiten Datenverarbeitungsanlage (14) überprüft.
- 20 15. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass als Hardwaremerkmal der zweiten Datenverarbeitungsanlage (14) eine vom Benutzer nicht änderbare Hardwareinformation der zweiten Datenverarbeitungsanlage (14) genutzt wird, insbesondere eine Seriennummer einer CPU oder eines Prozessors.
- 30 16. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass die zweiten Daten mit Hilfe einer Authentifizierungsprozedur verarbeitet werden, die dritte Informationen erzeugt, wobei die dritten Informationen insbesondere ein Verfallsdatum und Zugriffsrechte
- 35 der zweiten Datenverarbeitungsanlage (14) enthalten.

- 5 17. Verfahren nach Anspruch 16, dadurch gekennzeichnet, dass die Authentifizierungsprozedur bei der Verarbeitung von mehreren zweiten Daten unterschiedlicher zweiter Datenverarbeitungsanlagen (14) dieselben dritten Daten erzeugt.
- 10 18. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass die Überprüfung der Authentizität der zweiten Datenverarbeitungsanlage (14) mit Hilfe einer Challenge-/Response-Prozedur erfolgt.
- 15 19. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass die zweiten Daten ein signiertes Zertifikat enthalten.
- 20 20. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass die zweiten Daten einen Schlüssel enthalten, und dass die Authentifizierungsinformationen einen Authentifizierungscode enthalten, der mit Hilfe des Schlüssels (12) erzeugt wird.
21. Anordnung zum Erzeugen von Authentifizierungsinformationen,
- bei der eine erste Datenverarbeitungsanlage (16) eine erste Information erzeugt, wobei die erste Information einer zweiten Datenverarbeitungsanlage (14) einer Bedieneinheit zugeführt wird,
- 30 die zweite Datenverarbeitungsanlage (14) mit Hilfe der ersten Information und einer in der zweiten Datenverarbeitungsanlage (14) enthaltenen weiteren Information erste Daten erzeugt,
- 35 eine Datenleitung vorgesehen ist, über die erste Daten von der ersten Datenverarbeitungsanlage (16) zur zweiten Datenverarbeitungsanlage (14) übertragbar sind,

die zweite Datenverarbeitungsanlage (14) abhängig von den ersten Daten zweite Daten erzeugt,

5 die zweiten Daten über die Datenleitung von der zweiten Datenverarbeitungsanlage (14) zur ersten Datenverarbeitungsanlage (16) übertragbar sind,

10 und bei der die zweite Datenverarbeitungsanlage (14) mit Hilfe der zweiten Daten Authentifizierungsinformationen zur Authentifizierung der zweiten Datenverarbeitungsanlage (40) erzeugt.

15 22. Verfahren zur Authentifizierung einer Bedieneinheit eines elektrofotografischen Druck- oder Kopiersystems,

bei dem in einer ersten Datenverarbeitungsanlage (14) der Bedieneinheit erste Daten gespeichert werden,

20 die erste Datenverarbeitungsanlage (14) mit Hilfe der ersten Daten eine Authentifizierungsinformation erzeugt, die mit Hilfe von Authentifizierungsdaten zu einer zweiten Datenverarbeitungsanlage (40) des Druck- oder Kopiersystems übertragen werden,

die Authentizität der ersten Datenverarbeitungsanlage (14) durch die zweite Datenverarbeitungsanlage (40) überprüft wird,

30 und bei dem mit Hilfe der Authentifizierungsdaten durch die zweite Datenverarbeitungsanlage (40) Zugriffsrechte der ersten Datenverarbeitungsanlage (14) festgelegt werden.

35 23. Verfahren nach Anspruch 22, dadurch gekennzeichnet, dass die ersten Daten einen Schlüssel (12) und/oder eine Signatur enthalten.

24. Verfahren nach Anspruch 23, dadurch gekennzeichnet, dass der Schlüssel (12) ein Public-Key und/oder ein Private-Key ist.

5

25. Verfahren nach einem der Ansprüche 22 bis 24, dadurch gekennzeichnet, dass die Daten zwischen der ersten Datenverarbeitungsanlage (14) und der zweiten Datenverarbeitungsanlage (40) mit Hilfe einer Netzwerkverbindung übertragen werden, wobei die erste Datenverarbeitungsanlage (16) zur Fernbedienung, Fernwartung und/oder Ferndiagnose des Druck- oder Kopiersystems dient und zumindest Zugriff auf Steuereinheiten des Druck- oder Kopiersystems nach dem Überprüfen der Authentizität hat.

10

15

26. Anordnung zum Authentifizieren einer Bedieneinheit eines elektrofotografischen Druck- oder Kopiersystems,

20

bei der eine erste Datenverarbeitungsanlage (14) der Bedieneinheit erste Daten enthält,

die erste Datenverarbeitungsanlage (14) mit Hilfe der ersten Daten eine Authentifizierungsinformation erzeugt,

die erste Datenverarbeitungsanlage (14) die Authentifizierungsinformationen mit Hilfe von Authentifizierungsdaten zu einer zweiten Datenverarbeitungsanlage (40) des Druck- oder Kopiersystems überträgt,

30

die zweite Datenverarbeitungsanlage (40) mit Hilfe der Authentifizierungsdaten die Authentizität der ersten Datenverarbeitungsanlage (14) überprüft,

35

und bei der die zweite Datenverarbeitungsanlage (40) mit Hilfe der Authentifizierungsdaten Zugriffsrechte der ersten Datenverarbeitungsanlage (14) festlegt.

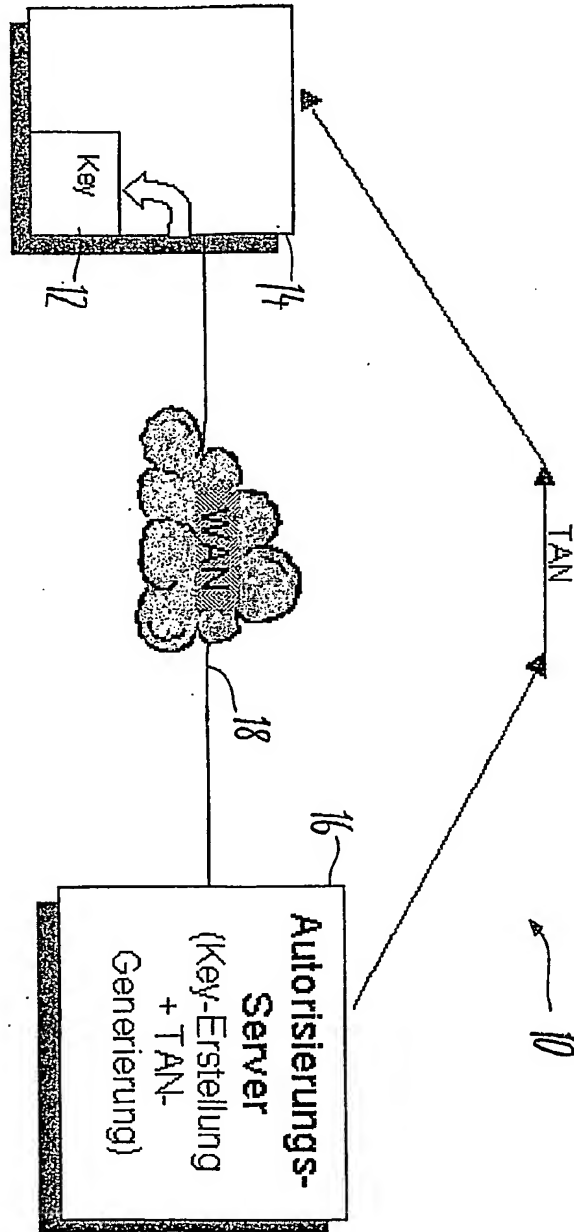
Zusammenfassung

Verfahren und Anordnung zum Authentifizieren einer Bedieneinheit sowie Übertragen einer Authentifizierungsinformation zu
5 der Bedieneinheit

Die Erfindung betrifft ein Verfahren und eine Anordnung zum Erzeugen von Authentifizierungsinformationen. Eine erste Datenverarbeitungsanlage (16) erzeugt eine erste Information,
10 wobei die erste Information einer zweiten Datenverarbeitungsanlage (14) einer Bedieneinheit zugeführt wird. Die zweite Datenverarbeitungsanlage (14) erzeugt mit Hilfe der ersten Informationen einer in der Datenverarbeitungsanlage (14) enthaltenen weiteren Information erste Daten. Die ersten
15 Daten werden von der ersten Datenverarbeitungsanlage (16) zur zweiten Datenverarbeitungsanlage (14) mit Hilfe einer Datenleitung übertragen. Die erste Datenverarbeitungsanlage (16) erzeugt abhängig von den ersten Daten zweite Daten. Die zweiten Daten werden von der ersten Datenverarbeitungsanlage (16)
20 zur zweiten Datenverarbeitungsanlage (14) übertragen. Die zweite Datenverarbeitungsanlage (14) erzeugt mit Hilfe der zweiten Daten Authentifizierungsinformationen zur Authentifizierung der zweiten Datenverarbeitungsanlage (14). Ferner betrifft die Erfindung ein Verfahren und eine Anordnung zur Authentifizierung einer Bedieneinheit eines elektrofotografischen Druck- oder Kopiersystems.

(Figur 1)

ZUSAMMENFASSUNG



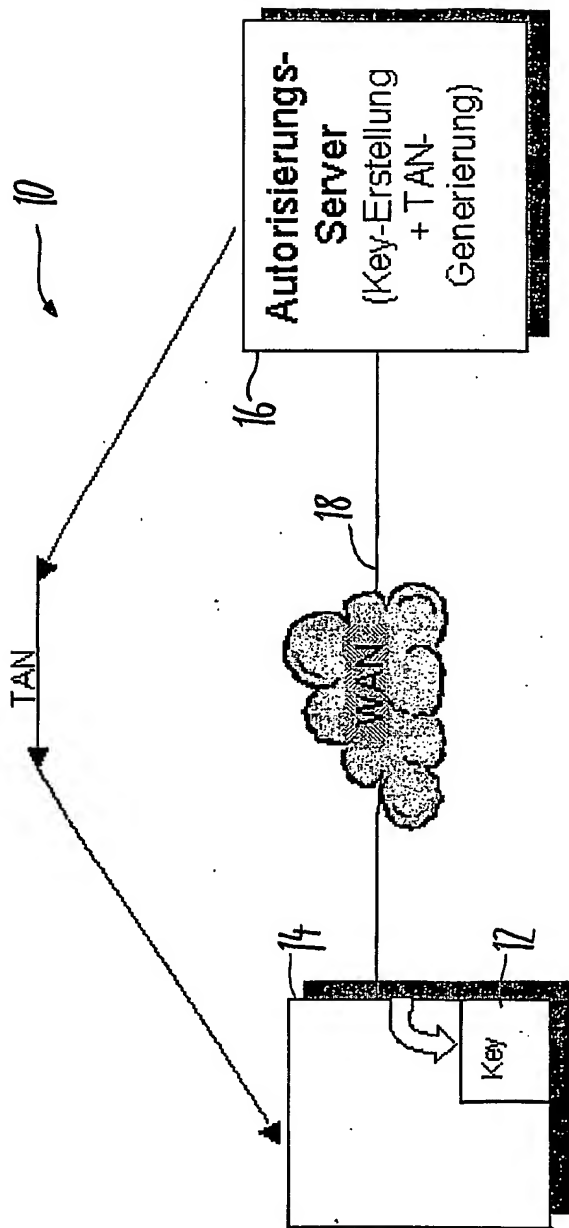


Fig. 1

20

24

26

28

30

32

34

36

38

22

21

23

25

27

29

31

33

35

37

39

40

41

42

43

44

45

46

47

48

49

50

51

52

53

54

55

56

57

58

59

60

61

62

63

64

65

66

67

68

69

70

71

72

73

74

75

76

77

78

79

80

81

82

83

84

85

86

87

88

89

90

91

92

93

94

95

96

97

98

99

100

101

102

103

104

105

106

107

108

109

110

111

112

113

114

115

116

117

118

119

120

121

122

123

124

125

126

127

128

129

130

131

132

133

134

135

136

137

138

139

140

141

142

143

144

145

146

147

148

149

150

151

152

153

154

155

156

157

158

159

160

161

162

163

164

165

166

167

168

169

170

171

172

173

174

175

176

177

178

179

180

181

182

183

184

185

186

187

188

189

190

191

192

193

194

195

196

197

198

199

200

201

202

203

204

205

206

207

208

209

210

211

212

213

214

215

216

217

218

219

220

221

222

223

224

225

226

227

228

229

230

231

232

233

234

235

236

237

238

239

240

241

242

243

244

245

246

247

248

249

250

251

252

253

254

255

256

257

258

259

260

261

262

263

264

265

266

267

268

269

270

271

272

273

274

275

276

277

278

279

280

281

282

283

284

285

286

287

288

289

290

291

292

293

294

295

296

297

298

299

300

301

302

303

304

305

306

307

308

309

310

311

312

313

314

315

316

317

318

319

320

321

322

323

324

325

326

327

328

329

330

331

332

333

334

335

336

337

338

339

340

341

342

343

344

345

346

347

348

349

350

351

352

353

354

355

356

357

358

359

360

361

362

363

364

365

366

367

368

369

370

371

372

373

374

375

376

377

378

379

380

381

382

383

384

385

386

387

388

389

390

391

392

393

394

395

396

397

398

399

400

401

402

403

404

405

406

407

408

409

410

411

412

413

414

415

416

417

418

419

420

421

422

423

424

425

426

427

428

429

430

431

432

433

434

435

436

437

438

439

440

441

442

443

444

445

446

447

448

449

450

451

452

453

454

455

456

457

458

459

460

461

462

463

464

465

466

467

468

469

470

471

472

473

474

475

476

477

478

479

480

481

482

483

484

485

486

487

488

489

490

491

492

493

494

495

496

497

498

499

500

501

502

503

504

505

506

507

508

509

510

511

512

513

514

515

516

517

518

519

520

521

522

523

524

525

526

527

528

529

530

531

532

533

534

535

536

537

538

539

540

541

542

543

544

545

546

547

548

549

550

551

552

553

554

555

556

557

558

559

560

561

562

563

564

565

566

567

568

569

570

571

572

573

574

575

576

577

578

579

580

581

582

583

584

585

586

587

588

589

590

591

592

593

594

595

596

597

598

599

600

601

602

603

604

605

606

607

608

609

610

611

612

613

614

615

616

617

618

619

620

621

622

623

624

625

626

627

628

629

630

631

632

633

634

635

636

637

638

639

640

641

642

643

644

645

646

647

648

649

650

651

652

653

654

655

656

657

658

659

660

661

662

663

664

665

666

667

668

669

670

671

672

673

674

675

676

677

678

679

680

681

682

683

684

685

686

687

688

689

690

691

692

693

694

695

696

697

698

699

700

701

702

703

704

705

706

707

708

709

710

711

712

713

714

715

716

717

718

719

720

721

722

723

724

725

726

727

728

729

730

731

732

733

734

735

736

737

738

739

740

741

742

743

744

745

746

747

748

749

750

751

752

753

754

755

756

757

758

759

760

761

762

763

764

765

766

767

768

769

770

771

772

773

774

775

776

777

778

779

780

781

782

783

784

785

786

787

788

789

790

791

792

793

794

795

796

797

798

799

800

801

802

803

804

805

806

807

808

809

810

811

812

813

814

815

816

817

818

819

820

821

822

823

824

825

826

827

828

829

830

831

832

833

834

835

836

837

838

839

840

841

842

843

844

845

846

847

848

849

850

851

852

853

854

855

856

857

858

859

860

861

862

863

864

865

866

867

868

869

870

871

872

873

874

875

876

877

878

879

880

881

882

883

884

885

886

887

888

889

890

891

892

893

894

895

896

897

898

899

900

901

902

903

904

905

906

907

908

909

910

911

912

913

914

915

916

917

918

919

920

921

922

923

924

925

926

927

928

929

930

931

932

933

934

935

936

937

938

939

940

941

942

943

944

945

946

947

948

949

950

951

952

953

954

955

956

957

958

959

960

961

962

963

964

965

966

967

968

969

970

971

972

973

974

975

976

977

978

979

980

981

982

983

984

985

986

987

988

989

990

991

992

993

994

995

996

997

998

999

1000

1001

1002

1003

1004

1005

1006

1007

1008

1009

1010

1011

1012

1013

1014

1015

1016

1017

1018

1019

1020

1021

1022

1023

1024

1025

1026

1027

1028

1029

1030

1031

1032

1033

1034

1035

1036

1037

1038

1039

1040

1041

1042

1043

1044

1045

1046

1047

1048

1049

1050

1051

1052

1053

1054

1055

1056

1057

1058

1059

1060

1061

1062

1063

1064

1065

1066

1067

1068

1069

1070

1071

1072

1073

1074

1075

1076

1077

1078

1079

1080

1081

1082

1083

1084

1085

1086

1087

1088

1089

1090

1091

1092

1093

1094

1095

1096

1097

1098

1099

1100

1101

1102

1103

1104

1105

1106

1107

1108

1109

1110

1111

1112

1113

1114

1115

1116

1117

1118

1119

1120

1121

1122

1123

1124

1125

1126

1127

1128

1129

1130

1131

1132

1133

1134

1135

1136

1137

1138

1139

1140

1141

1142

1143

1144

1145

1146

1147

1148

1149

1150

1151

1152

1153

1154

1155

1156

1157

1158

1159

1160

1161

1162

1163

1164

1165

1166

1167

1168

1169

1170

1171

1172

1173

1174

1175

1176

1177

1178

1179

1180

1181

1182

1183

1184

1185

1186

1187

1188

1189

1190

1191

1192

1193

1194

1195

1196

1197

1198

1199

1200

1201

1202

1203

1204

1205

1206

1207

1208

1209

1210

1211

1212

1213

1214

1215

1216

1217

1218

1219

1220

1221

1222

1223

1224

1225

1226

1227

1228

1229

1230

1231

1232

1233

1234

1235

1236

1237

1238

1239

1240

1241

1242

1243

1244

1245

1246

1247

1248

1249

1250

1251

1252

1253

1254

1255

1256

1257

1258

1259

1260

1261

1262

1263

1264

1265

1266

1267

1268

1269

1270

1271

1272

1273

1274

1275

1276

1277

1278

1279

1280

1281

1282

1283

1284

1285

1286

1287

1288

1289

1290

1291

1292

1293

1294

1295

1296

1297

1298

1299

1300

1301

1302

1303

1304

1305

1306

1307

1308

1309

1310

1311

1312

1313

1314

1315

1316

1317

1318

1319

1320

1321

1322

1323

1324

1325

1326

1327

1328

1329

1330

1331

1332

1333

1334

1335

1336

1337

1338

1339

1340

1341

1342

1343

1344

1345

1346

1347

1348

1349

1350

1351

1352

1353

1354

1355

1356

1357

1358

1359

1360

1361</

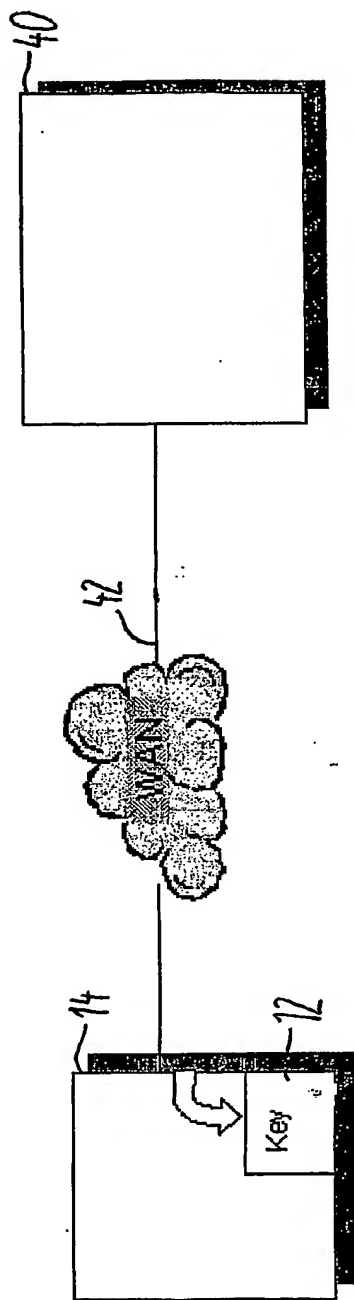


Fig. 3

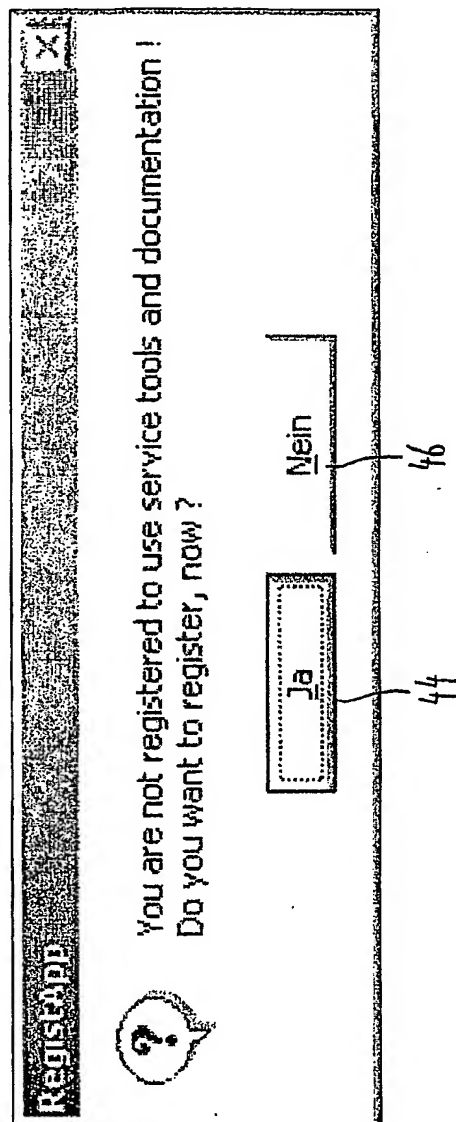


Fig. 4